REMARKS

Claims 1, 9 and 24 have been amended. No new matter is presented by these amendments.

Rejections Under 35 USC 102

The Applicant respectfully requests reconsideration of the rejection of claims 1-6, 8-13, 15, 16, and 24 under 35 USC 102(e) as being anticipated by *Ohmori et al.* ("*Ohmori*") (US 7,020,636). As explained in further detail below, *Ohmori* does not teach each and every feature of the independent claims, as amended herein.

Ohmori teaches a DVD rental system in which an IC card is utilized to facilitate decryption of encrypted content on a DVD. In *Ohmori's* first embodiment, a device key is written to the IC card during manufacture of the IC card. A DVD disc containing encrypted content includes a title key which has been encrypted with the device key. When a user wishes to rent the DVD disc, the user must present the IC card and the DVD disc together for processing by a shop apparatus (a computer system). A barcode is read from the DVD package which enables generation of a title ID. And after insertion of the IC card into a card reader in the shop apparatus, the rental process only proceeds after mutual authentication of the IC card with the shop apparatus. Assuming this to be the case, then a member number is read from the IC card. Use management information including rental start and end dates and the title ID are written to the IC card by the shop apparatus.

In order to decrypt the encrypted content on the DVD, the user first inserts both the DVD and the IC card in a DVD player having a reader for the IC card. Again, mutual authentication of the IC card with the DVD player is required in order to continue the process. After checking that the current date is within the range of the rental start and end times, the

encrypted title key is read from the DVD player and outputted to the IC card. The IC card utilizes its stored device key to decrypt the encrypted title key, thereafter outputting the decrypted title key to the DVD player. The DVD player then uses the decrypted title key to decrypt the encrypted content of the DVD.

In contrast to *Ohmori,* Applicant's claim 1 recites a method for controlling access to computer readable media wherein a digital authentication ticket is saved to a client device. In particular, the claimed digital authentication ticket includes a digital code, the digital code being separate from the particular computer readable content to enable receipt of the digital authentication ticket independent of a location of the particular computer readable content.

Ohmori fails to teach a digital code separate from the computer readable content to enable receipt of the digital authentication ticket independent of a location of the computer readable content. The Office apparently equates *Ohmori's* title key as being equivalent to the claimed digital code. However, in *Ohmori's* first embodiment, the title key is stored in encrypted form *on the DVD disc.* Only when both the DVD and the IC card are both inserted in the DVD player to ensure that the title ID stored in the IC card corresponds to that of the DVD disc, is the encrypted title key received by the IC card. As noted above, the IC card utilizes its device key to decrypt the encrypted title key, and outputs the decrypted title key to the DVD player for use in decrypting the encrypted content of the DVD. This entire sequence of operations requires that the DVD and IC card be present together in the same DVD player. As such, transference of *Ohmori's* title key, whether in encrypted or decrypted form, is not independent of the location of the DVD, thus failing to meet the limitation of Applicant's claim which specifies receipt of a digital authentication ticket independent of the location of computer readable content.

Even considering *Ohmori's* device key as possibly equivalent to Applicant's claimed digital code, the reference nonetheless still does not teach or suggest the features of

Applicant's claim 1. *Ohmori's* device key is written to the IC card at the time of manufacture and never transferred to the DVD player, whereas Applicant's claim 1 recites wireless transfer of a digital authentication ticket from a client device to a computer system. In fact, *Ohmori's* IC card and device key are part of a copyright protection system diverted for use in a rental system. Apparently, the device key is tied to the IC card and intentionally not transferrable, as this promotes copyright protection, and *Ohmori* does not teach transfer of the device key.

In a second embodiment, *Ohmori* teaches storage of the encrypted title key to the IC card by the shop apparatus. However, in order to receive the encrypted title key, both the DVD and IC card must be present at the shop apparatus. The IC card must mutually authenticate with the shop apparatus, and further output a device key identifier, and the bar code of the DVD must be read to determine the proper title ID so as to obtain the proper encrypted title key for storage to the IC card. When a user later wishes to playback the encrypted content of the DVD, a procedure similar to that of the first embodiment is followed (except that the encrypted title key is already stored on the IC card), requiring insertion of both the DVD and the IC card in the same DVD player. Thus, as in *Ohmori's* first embodiment, transfer of the title key both to and from the IC card, in encrypted and decrypted forms, respectively, requires that the DVD be present at the same time.

In sum, the *Ohmori* reference teaches transfer of a title key that is dependent on the location of the corresponding DVD disc. In contrast, Applicant's claim 1 is directed to a digital authentication ticket that can be received independent of the location of its corresponding computer readable content.

Additionally, Applicant has amended claim 1 to recite that the client device obtains the digital authentication ticket via a communication network, the client device being capable of obtaining the digital authentication ticket anywhere the client device has access to the

communication network. As discussed above, *Ohmori* does not teach receipt of a digital authentication ticket independent of the location of corresponding computer readable content. As such, neither does *Ohmori* teach obtaining the digital authentication ticket anywhere the client device has access to a communication network, as *Ohmori* requires proximity of its IC card and DVD disc.

In view of the above, it is respectfully submitted that Applicant's claim 1 is not anticipated by the *Ohmori* reference. Likewise, independent claims 9 and 24 are not anticipated by *Ohmori* for at least the same reasons as those discussed with regard to claim 1. Dependent claims 2-6, 8, 10-13, 15, and 16 and are believed to be patentable over *Ohmori* for at least the same reasons as the independent claims.

Rejections under 35 USC 103

Applicant respectfully requests reconsideration of the rejections of claims 1-6, 8-13, 15, 16, and 24 under 35 USC 103(a) as being unpatentable over *Ohmori*, and the rejection of claim 17 as being unpatentable over *Ohmori* in view of *Ginter et al.* ("*Ginter*") (US 5,892,900). The deficiencies of the *Ohmori* reference have been discussed above in regards to the rejections under Section 102. Neither the Examiner's alternative position regarding inherency of *Ohmori* nor the addition of the *Ginter* reference cures the deficiencies of the *Ohmori* reference as previously discussed. Therefore, the Office is respectfully requested to withdraw the rejections under Section 103.

Conclusion

In view of the foregoing remarks and the amendments to the claims, it is submitted that the pending claims are in condition for allowance. If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 749-6903. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No SONYP026).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

/Albert S. Penilla/

Albert S. Penilla, Esq.
Reg. No. 39,487

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Facsimile: (408) 749-6901